ABSTRACT OF THE DISCLOSURE

The present invention provides a method for reliably carrying out an encryption level evaluation process in a common-key block encryption method. To be more specific, an algorithm of a key-scheduling part is expressed in terms of equations represented by vectors and a matrix, and non-linear transformation output values and initial values are eliminated from the matricial equation by carrying out a unitary transformation process in order to find all equations expressing linear relations among round keys. In accordance with the method, it is possible to comprehend all equations expressing linear relations among round keys in the common-key block encryption method without regard to the complexity of key scheduling and evaluate the encryption level of the common-key block encryption method on the basis of the derived equations expressing linear relations among round keys.